AMENDMENT TO THE CLAIMS

The following claim listing replaces all prior listings and versions of the claims:

LISTING OF CLAIMS

1. (Currently Amended) A method for securely distributing a component from a network host to a network appliance, the method comprising [[the]] steps of:

executing a secure kernel on said network appliance, said secure kernel including boot code for allowing said network appliance to initially boot up and establish communication with said network host;

~~signing, by said network host,~~ determining, by said secure kernel, whether a configuration file exists on said network appliance, said configuration file being signed by said network host and including a load table which defines a plurality of authorized components for said network appliance;

~~executing a secure kernel and said signed configuration file on said network appliance, said secure kernel including computer code for checking the authenticity of said configuration file and boot code for allowing said network appliance to initially boot up and establish communication with said network host;~~

upon determining that said configuration file exists on said network appliance, verifying, by said secure kernel, the authenticity of said configuration file;

only upon verifying that said configuration file is authenticated, reading, by said secure kernel, said load table ~~only after said verifying step~~; and

loading said plurality of authorized components defined in said load table onto said network appliance~~,~~

~~wherein said network appliance is determined to be authorized receive said authorize~~

~~components~~.

2. (Original) The method of claim 1, wherein said loading step comprises loading an operating system.

3. (Original) The method of claim 1, wherein said loading step comprises loading a computer software application.

4. (Original) The method of claim 1, wherein said loading step comprises loading services.

5. (Currently Amended) The method of claim 1, ~~further comprising the steps of:~~ wherein:

in the step of verifying, when said secure kernel judged that said configuration file is not authenticated, the method further comprises steps of:

requesting, by said secure kernel, an updated configuration file;

generating, by said host, [[an]] said updated configuration file;

signing, by said host, said updated configuration file; and

transmitting said signed updated configuration file from said host to said network appliance, and [[;]]

said secure kernel verifies ~~verifying, by said secure kernel,~~ the authenticity of said updated configuration file [[;]] and ~~thereafter reading, by said secure kernel,~~ read said updated configuration file.

6. (New) The method of claim 1, wherein:

in the step of determining, when said secure kernel determined that a configuration file does not exist on said network appliance, the method further comprises steps of:

requesting, by said secure kernel, a new configuration file;

generating, by said host, said new configuration file;

signing, by said host, said new configuration file; and

transmitting said signed new configuration file from said host to said network appliance, and

said secure kernel verifies the authenticity of said new configuration file and read said new configuration file.

7. (New) The method of claim 1, wherein said plurality of authorized components include a hardware component.

8. (New) The method of claim 1, wherein said load table describes souses of the plurality of authorized components.

9. (New) The method of claim 1, wherein in the step of loading, when said secure kernel fails to properly load all of the plurality of authorized components defined in said load table onto said network appliance, said secure kernel sends a request through said network for any authorized component which is not properly loaded.

10. (New) The method of claim 9, wherein:

said configuration file includes information regarding sources of said authorized components specified in said load table, and

said secure kernel sends said request to a souse included in said information.

11. (New) The method of claim 1, wherein:

said network appliance is a set top box, and

said authorized components relates to a television program.

12. (New) The method of claim 1, wherein said secure kernel is stored in a non-volatile memory which is protected from an access of a user of said network appliance.